

STATUS OF CLAIMS

Claims 1 - 28 are pending.

Claims 1 – 28 stand rejected.

Claims 1 – 4 have been amended without prejudice herein.

Claims 11 – 28 have been cancelled without prejudice herein.

REMARKS

Claim Amendments

Claims 11 – 28 have been cancelled, without prejudice, to speed prosecution of the present application. Applicant reserves the right to re-introduce these, and/or analogous, claims in the present or a related application.

Claims 1 – 4 have been amended, without prejudice, to more clearly recite aspects of the present invention. For example, Claim 1 has been amended to recite:

A method for facilitating secure communications among at least two parties over a communication network, comprising:

retaining a first private key and transmitting a corresponding first initial public key and synchronizing indicator;

using a received second public key and second synchronizing indicator in combination with said retained first private key to determine, and retain, a first encryption key;

determining a second private key, a third public key and a third synchronizing indicator, wherein said second private key is retained with said first retained private key;

encrypting at least said third synchronizing indicator using said first encryption key;

transmitting said third public key and encrypted third synchronizing indicator;

decrypting a received fourth synchronizing indicator using said first encryption key; and

determining a second encryption key from said second private key, a fourth public key and said decrypted fourth synchronizing indicator, wherein said second encryption key is retained with said first encryption key.

Applicant submits support for amended Claim 1 may be found in the specification as originally filed, such that no new matter has been introduced. By way of non-limiting example only, reference may be drawn to the original Claim 1, and in the specification in Table 1 and the example immediately following on pages 9 and 10 of the original application.

Therein, there is disclosed a method for sharing encryption keys (E_{A1} , E_{A2} ...) among at least two parties (Party A and Party B). The encryption keys are useful for facilitating secure communications between the two parties. *See, e.g., Specification, page 1, lines 5 - 12.* The disclosed method includes Party A retaining a first private key (P_{RA1}) and transmitting a first public key and synchronizing indicator (P_{KA1} , MI_{A1}). Party A uses a received second public key (P_{KB1}) and synchronizing indicator (MI_{B1}) in combination with the first private key (P_{RA1}) to determine, and retain, an initial encryption key (E_{A1}).

Party A determines a second private key (P_{RA2}), and a third public key and synchronizing indicator (P_{KA2} , MI_{A2}), wherein the second private key (P_{RA2}) is retained among the retained next private keys. Party A encrypts the third synchronizing indicator (MI_{A2}) using the first encryption key (E_{A1}). Party A transmits the encrypted third synchronizing indicator ($E_{A1}(MI_{A2})$) over the network.

Party A decrypts a received fourth synchronizing indicator ($E_{B1}(MI_{B2})$) using the first encryption key (E_{A1}). Finally, Party A determines a second encryption key (E_{A2})

from the second private key (P_{RA2}), a fourth public key (P_{KB2}) and the decrypted fourth synchronizing indicator (MI_{B2}), wherein the next encryption key (E_{A2}) is retained among the retained encryption keys (e.g., with E_{A1}).

35 U.S.C. 103(a) Rejections

Claims 1 – 28 were rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro (United States Patent No. 6,009,176) in view of Bjerrum (United States Patent No. RE.36,310). Applicant respectfully requests reconsideration and removal of these rejections for at least the following reasons.

35 U.S.C. §103(a) sets forth in part:

[a] patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.

To establish a prima facie case of obviousness, all of the recited claim limitations must be taught or suggested in the prior art. *See, MPEP 2143.03; see also, In re. Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974)*. Further, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine reference teachings. *See, M.P.E.P. 706.02(j)*. Further yet, the teaching or suggestion to make the claimed combination must be found in the prior art, and not based on the applicant's own disclosure. *In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)*. Applicant respectfully submits the cited art fails to teach

each of the recited limitations of any of the claims, and that even if the references when combined did teach all of the recited limitations, a proper motivation for combining the references as argued is lacking.

Referring first to Claim 1, the present claim recites in part, “determining a second encryption key from said second private key, a fourth public key and said decrypted fourth synchronizing indicator, wherein said second encryption key is retained with said first encryption key.” Gennaro and Bjerrum fail, in any combination, to teach this recited limitation.

The Office action dated March 23, 2005 acknowledges that Genarro fails to teach determining and retaining a next encryption key. *See, 3/23/2005 Office action, par. 5.* Further, Genarro clearly fails to teach determining a second encryption key from a second private key, a fourth public key and a decrypted fourth synchronizing indicator as recited in present Claim 1. The Office action attempts to remedy this admitted shortcoming of Genarro by importing select teachings of Bjerrum. *See, 3/23/2005 Office action, pars. 6 and 7.*

More particularly, the Office action argues Bjerrum teaches determining a next encryption key from said received information item, wherein the next encryption key is retained among other encryption keys in col. 37, lines 52-56. *See, 3/23/2005 Office action, par. 6.* Applicant traverses this assertion. This selected excerpt of Bjerrum clearly fails to teach, or suggest, determining a second encryption key *from a second private key, a fourth public key and a decrypted fourth synchronizing indicator* as is recited by present Claim 1. In contrast, Bjerrum merely teaches decrypting an encrypted combination of two random numbers (the claimed

third authenticity message to obtain the claimed second combination of the claimed second and third random numbers). *See, U.S. Pat. No. Re. 36,310, Claim 31.*

Accordingly, Applicant submits Bjerrum, like Genarro, fails to teach the recited limitations of determining a second encryption key from a second private key, a fourth public key and a decrypted fourth synchronizing indicator, as recited in present Claim 1.

Accordingly, as neither Genarro nor Bjerrum teach, or even suggests for that matter, determining a second encryption key from a second private key, a fourth public key and a decrypted fourth synchronizing indicator as is recited by present Claim 1, any combination thereof likewise fails to teach such limitations.

The above notwithstanding, Applicant submits a proper motivation for modifying Genarro to store multiple keys is lacking, at least by virtue that Genarro squarely teaches against retaining more than one encryption key – in at least that Genarro expressly teaches that once used on an i^{th} block, the $i-1^{\text{th}}$ secret key is destroyed. *See, U.S. Pat. No. 6,009,176, col. 7, lines 24 – 25.* The Genarro reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention. *See, W.L. Gore & Associates, Inc. v. Garlock, Inc., 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), cert. denied, 469 U.S. 851 (1984).* Thus, the fact that Genarro teaches to destroy an $i-1^{\text{th}}$ block after processing an i^{th} block must be considered when determining whether or not a proper motivation exists for modifying Genarro as argued in the Final Office action. As Genarro actually teaches away from the claimed invention – as Claim 1 expressly recites retaining multiple encryption keys – Applicant submits a proper motivation to

modify Genarro to contradict its express teaching to store only a single encryption key is lacking.

Further, while the referenced portion of Genarro claims decrypting an encrypted combination of two random numbers (the claimed third authenticity message to obtain the claimed second combination of the claimed second and third random numbers), this does not change the fact that Bjerrum itself expressly teaches that the object of its invention is to “provide a method ... , according to which method it is possible to establish immediately a secure data or document transfer between two computer systems without having to exchange encryption/decryption keys between the computer systems, reveal details concerning security levels, etc., and according to which method it is ensured that the desired data or document transfer actually takes place, as it is ensured that it will not be possible for either of the parties or for a third party to interfere with the data or document transfer. *See, Col. 2, lines 5 – 14.*

As this passage demonstrates, Bjerrum thus teaches the skilled artisan the undesirability of and a secure data transfer method that avoids exchanging encryption/decryption keys between computer systems. Thus, Bjerrum, properly considered in its entirety, teaches away from the use of exchanged security information. Accordingly, Applicant submits a proper motivation for combining the teachings of Gennaro, which uses exchanged information, and Bjerrum, which teaches against using exchanged information, to reach the claimed invention is also lacking.

Accordingly, Applicant respectfully requests reconsideration and removal of the rejection of Claim 1 for at least the reasons set forth above, namely, that a proper motivation for combining the references to meet the claimed invention is lacking. Applicant also respectfully requests reconsideration and removal of the rejections of Claims 2 – 10 as well, at least by virtue of these claims' ultimate dependency upon a patentably distinct base Claim 1.


CONCLUSION

Applicant believes he has addressed all outstanding grounds raised in the outstanding Office action, and respectfully submits the present case is in condition for allowance, early notification of which is earnestly solicited.

Should there be any questions or outstanding matters, the Examiner is cordially invited and requested to contact Applicant's undersigned attorney at his number listed below.

Dated: July 25, 2005

Respectfully submitted,



Edward J. Howard
Registration No. 42,670

Plevy, Howard & Darcy, P.C.
PO Box 226
Fort Washington, PA 19034
Tel: (215) 542-5824
Fax: (215) 542-5825